

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for detecting an intrusion detection initiated in a first network toward a second network, comprising:

receiving, at a probe located outside the second network, data packets communicated over a first network link which transmits, from the first network to the second network, the data packets in a format suitable for the first network;

converting the received data packets received at the probe into a format suitable for an intrusion detection system (IDS) for detecting the intrusion initiated in the first network toward the second network, the IDS located outside the second network and configured to not receive data packets exchanged inside the second network a-second-network-link;

monitoring, by the probe, the received data packets received at the probe to evaluate network performance of the first network link;

collecting, by the probe, current network performance data based on the network performance;

updating, by the probe, historical network performance information with the current network performance data; and

transmitting, by the probe over a second network link to the IDS data-converted the converted data packets and the updated historical

network performance information, ~~to an intrusion detection system in communication with the second network link~~, wherein at least one of the ~~data converted~~ converted data packets and the updated historical network performance information is used by the IDS ~~intrusion detection system~~ to detect ~~[[an]] the~~ intrusion ~~on the first network link~~.

2. (Currently Amended) The method of claim 1 wherein the first network link is includes a wide area network WAN link and the second network link is includes a local area network [[LAN]].
3. (Currently Amended) The method of claim 1 wherein the method further comprises receiving, at ~~[[a]] the~~ probe, data packets communicated over a third network link which transmits, from the first network to the second network, data packets in a format suitable for the first network.
4. (Previously Presented) The method of claim 3, further comprising the step of aggregating the data packets received over the first network link and the data packets received over the third network link, wherein the aggregated data packet appears to emanate from a single logical source.
5. (Original) The method of claim 1 wherein the first network link operates using at least one HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.

6. (Original) The method of claim 1 wherein the first network link comprises a protocol that encapsulates data traffic.
7. (Original) The method of claim 6 wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.
8. (Currently Amended) The method of claim [[3]] 1, further comprising the step of maintaining, by the probe, an audit trail buffer for forensic analysis.
9. (Currently Amended) The method of claim 8 wherein the audit trail buffer comprises a memory for recording monitored data packets.
10. (Currently Amended) The method of claim [[9]] 3, further comprising the step of maintaining, by the probe, an audit trail buffer for forensic analysis, wherein the audit trail buffer comprises a memory for recording monitored data packets and wherein the memory records data packets from at least one of the first network link and the third network link.
11. (Currently Amended) The method of claim 8, further comprising the steps of: receiving, by the probe, an event notification; and upon receipt of the event notification, communicating, by the probe, [[the]] current contents of the audit trail buffer.
12. (Currently Amended) The method of claim 1, wherein the converting step comprises:

storing received the data packets received at the probe in a collection
buffer;

stripping header information associated with a protocol of the first network
link; and

adding header information associated with a protocol of the second network link.

13. (Currently Amended) The method of claim 12, wherein the step of storing comprises storing data packets received from at least one of the first network link and a third network link.

14. (Previously Presented) The method of claim 12 wherein:

the stripping step further comprises stripping checksum information
associated with the protocol of the first network link; and
the adding step further comprises adding checksum information
associated with the protocol of the second network link.

15. (Currently Amended) The method of claim 13, the step of stripping comprising ~~comprises~~ stripping at least one of a Layer 2 MAC header, an Ethernet source address, and an Ethernet destination address.

16-20. (Canceled).

21. (Currently Amended) A network performance probe system for detecting
an intrusion initiated in a first network toward a second network, the probe
system comprising:

- a first network interface for ~~monitoring~~ receiving data packets
communicated over a first network link which transmits, from the
first network to the second network, the data packets in a format
suitable for the first network, wherein the probe is located outside
the second network;
- a packet converter for converting the ~~monitored~~ data packets received at
the first network link into a format suitable for ~~a second network link~~
an intrusion detection system (IDS) for detecting the intrusion
initiated in the first network toward the second network, the IDS
located outside the second network and configured to not receive
data packets exchanged inside the second network;
- a protocol for collecting current network performance data related to the
first network link and updating historical network performance
information with the current network performance data; and
- a second network interface for communicating, over a second network link
to the IDS, the converted data packets and the updated historical
network performance information ~~to an intrusion detection system
in communication with the second network link~~, wherein at least
one of the ~~data-converted~~ the converted data packets and the
updated historical network performance information is used by the
IDS intrusion detection system to detect ~~[[an]] the intrusion on the
first network link.~~

22. (Currently Amended) The network performance probe system of claim 21 further comprising a third network interface for ~~monitoring~~ receiving data packets communicated over a third network link which transmits, from the first network to the second network, data packets in a format suitable for the first network.
23. (Currently Amended) The network performance probe system of claim 22 further comprising an aggregator for aggregating the data packets from the first network link and the data packets from the third network link, wherein the aggregated data packet appears to emanate from a single logical source.
24. (Currently Amended) The network performance probe system of claim 21 wherein the first network ~~[[link]]~~ comprises a wide area network ~~WAN~~ link and the second network ~~[[link]]~~ comprises an Ethernet network.
25. (Previously Presented) The network performance probe system of claim 21 wherein the first network link operates using at least one HSSI protocol, T1 protocol, E1 protocol, ATM, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, and 10G Ethernet protocol.
26. (Previously Presented) The network performance probe system of claim 21 wherein the first network link comprises a protocol that encapsulates data traffic.
27. (Previously Presented) The network performance probe system of claim 26 wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM

protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.

28. (Currently Amended) The network performance probe system of claim 21, further comprising a performance analyzer for acquiring network performance data in response to the ~~monitored data~~ packets received at the first network link ~~communicated~~ over the first network link.

29. (Currently Amended) The network performance probe system of claim ~~[[22]] 21, wherein the probe further comprises~~ comprising an audit trail buffer maintainable for forensic analysis.

30-31. (Canceled).

32. (Currently Amended) The network performance probe system of claim 29 wherein the audit trail buffer comprises a memory for recording ~~monitored data~~ packets received at the first network link for forensic analysis.

33. (Currently Amended) The network performance probe system of claim 32, ~~wherein the probe further comprises~~ comprising an event notification receiver for causing the probe, upon receipt of ~~[[the]]~~ an event notification, ~~to communicate a~~ communication of the current contents of the audit trail buffer.

34. (Currently Amended) The network performance probe system of claim 21, wherein the converter comprises:

a collection buffer for storing ~~received data~~ packets received at the first
network link;

a stripper for stripping header information associated with a protocol of the
first network link; and
an adder for adding header information associated with a protocol of the
second network link.

35-39. (Canceled).

40. (Currently Amended) An article of manufacture comprising a computer
program storage medium having computer readable program code embodied
therein for ~~providing~~ detecting an intrusion detection initiated in a first network
toward a second network, the computer readable program code in the article of
manufacture including:

computer readable code for causing a computer to receive, at a probe
located outside the second network, data packets communicated
over a first network link which transmits, from the first network to
the second network, the data packets in a format suitable for the
first network;

computer readable code for causing a computer to convert the received
data packets into a format suitable for an intrusion detection system
(IDS) for detecting the intrusion initiated in the first network toward
the second network, the IDS located outside the second network,
and configured to not receive data packets exchanged inside the
second network ~~a second network link~~;

computer readable code for causing a computer to monitor, via the probe, the received data packets to evaluate network performance of the first network link;

computer readable code for causing a computer to collect current network performance data based on the network performance;

computer readable code for causing a computer to update historical network performance information with the current network performance data; and

computer readable code for causing a computer to transmit, via the probe over a second network link to the IDS, ~~data-converted the converted data~~ packets and the updated historical network performance information ~~to an intrusion detection system in communication with the second network link~~, wherein at least one of the ~~data-converted~~ converted data packets and the updated historical network performance information is used by the IDS ~~intrusion detection system~~ to detect an the intrusion ~~on the first network link~~.

41. (Currently Amended) The article of manufacture of claim 40 wherein the computer program storage medium comprises at least one of a computer magnetic disk, a computer optical disk, a tape, a non-volatile memory, a system memory, and a computer hard drive.

42. (Currently Amended) A computer program storage medium readable by a computer, embodying a computer program of instructions executable by the

computer to perform method steps for providing detecting an intrusion detection initiated in a first network toward a second network, the method steps comprising:

receiving, at a probe located outside the second network, data packets communicated over a first network link which transmits, from the first network to the second network, the data packets in a format suitable for the first network;

converting the received data packets received at the probe into a format suitable for an intrusion detection system (IDS) for detecting the intrusion initiated in the first network toward the second network, the IDS located outside the second network and configured to not receive data packets exchanged inside the second network a-second-network-link;

monitoring, by the probe, the received data packets received at the probe to evaluate network performance of the first network link;

collecting, by the probe, current network performance data based on the network performance;

updating, by the probe, historical network performance information with the current network performance data; and

transmitting, by the probe over a second network link to the IDS, data-converted the converted data packets and the updated historical network performance information ~~to an intrusion detection system in communication with the second network link~~, wherein at least

one of the ~~data-converted~~ converted data packets and the updated historical network performance information is used by the IDS ~~intrusion detection system~~ to detect ~~[[an]]~~ the intrusion on the ~~first~~ network link.

43. (Currently Amended) The computer program storage medium of claim 42 further comprising at least one of a computer magnetic disk, a computer optical disk, a tape, a non-volatile memory, a system memory, and a computer hard drive.

44. (Currently Amended) The method of claim 1, wherein the historical network performance information comprises an historical traffic profile.

45. (Previously Presented) The method of claim 1, wherein the intrusion detection system uses the historical network performance information as a basis for an action.

46. (Previously Presented) The network performance probe system of claim 21, wherein the historical network performance information comprises a historical traffic profile.

47. (Previously Presented) The network performance probe system of claim 21, wherein the intrusion detection system uses the historical network performance information as a basis for an action.

48. (New) The method of claim 1, wherein the format suitable for the IDS is a format suitable for the second network.

49. (New) The network performance probe system of claim 21, wherein the format suitable for the IDS is a format suitable for the second network.
50. (New) The method of claim 1 further comprising, prior to transmitting over the second network link, filtering a subset of the converted data packets.
51. (New) The method of claim 50, wherein the filtering comprises filtering based on predetermined criteria or user-defined criteria.
52. (New) The network performance probe system of claim 21, further comprising a filter for filtering a subset of the converted data packets prior to communicating, over the second network link to the IDS, the converted data packets and the updated historical network performance information.
53. (New) The network performance probe system of claim 52, wherein the filtering of the subset of the converted data packets is based at least in part on predetermined criteria or user defined criteria.